

# CYBER THIEVES!

Using everything from Facebook to online offers, hi-tech criminals are always trying to con you. Here's how to protect yourself

BY MAX ALEXANDER

**Tom Farmer loves the way** Facebook helps him reconnect with old friends and former colleagues. So the 50-year-old communications consultant from Seattle was excited to get a live chat message from Elissa, a woman he had worked with some years previously. But after they exchanged pleasantries, the message quickly turned urgent. Elissa and a companion were in trouble in London.

"We were mugged at gunpoint last night," she wrote. "All cash, credit cards and phone were stolen."

"Holy moly," replied Farmer. "Anything I can do for you from here?"

It just so happened there was. "Could you please loan me some \$\$\$ to sort out the hotel bills and also take a cab to the airport," she wrote. "I will refund it tomorrow."

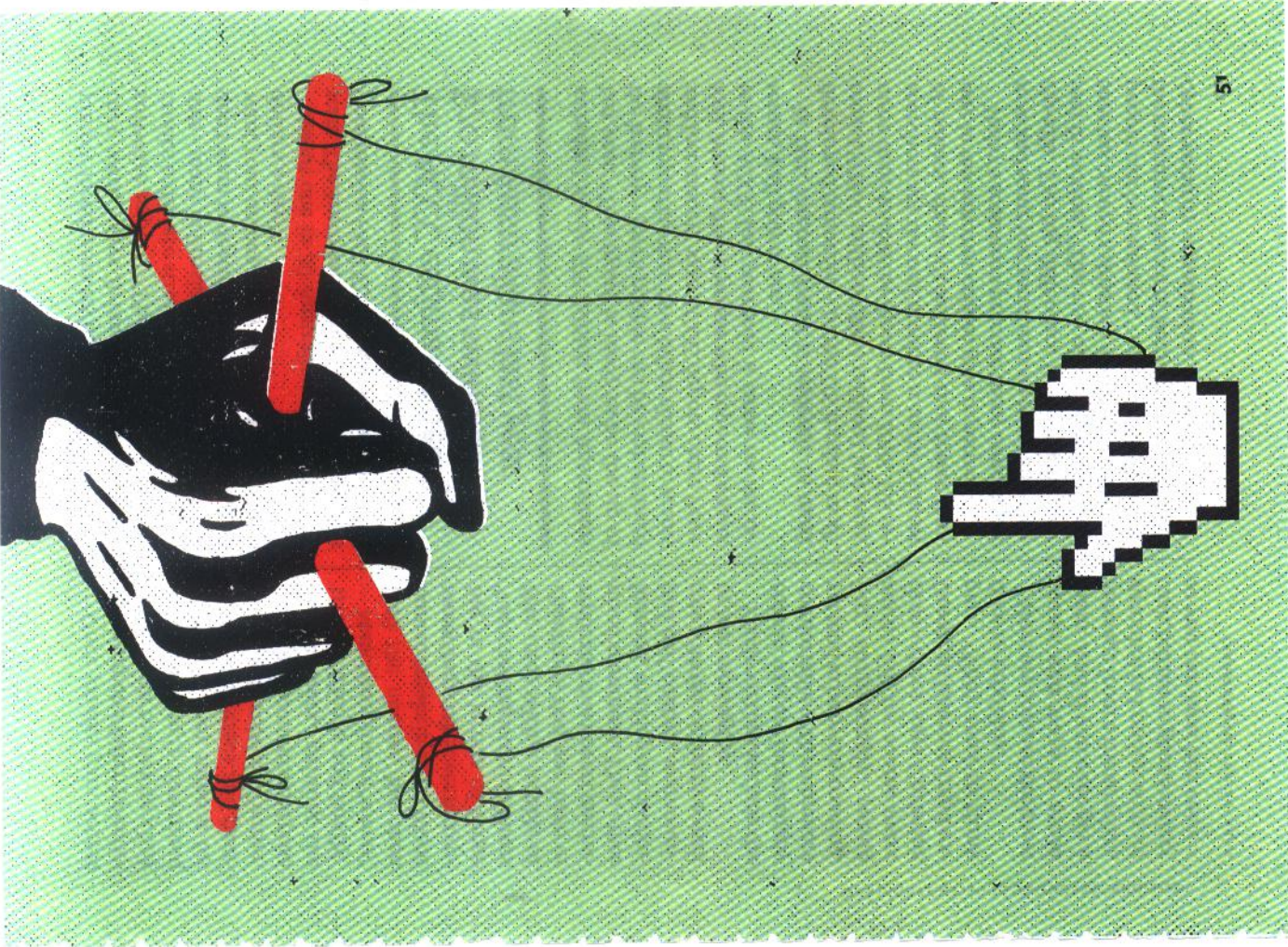
Farmer offered to phone the hotel and cover the bill with his credit card, but Elissa kept insisting on a wire transfer. That's when he grew suspicious. "Call me paranoid," he wrote back, "but what company were we working for when we met?"

After a long pause, Elissa answered correctly. Then Farmer realised that information could be gleaned from his Facebook profile. So he asked for the name of their former boss.

Silence.

At that point, the game was up. "Elissa", it turned out, was one of a new breed of internet crooks who use personal account information to trick you into thinking they are legitimate companies, services or even your friend.

And they are succeeding. "The bad guys used to be





pinply-faced teens trying to prove how smart they were," says Brian Yoder, an antivirus software expert. "The predominant online crooks today are straight-up organised criminals - many in Russia, Spain and Ukraine. They don't want to destroy your computer; they just want your money. They're making millions of dollars a day."

About one in 20 Australians is caught by a scam. The Australian Competition and Consumer Commission (ACCC) estimates that fraudsters

## The ACCC estimates nearly \$70 million was swindled from Australians last year

swindled nearly \$70 million from Australians last year. "This figure is likely to be the tip of the iceberg - given people can be embarrassed about reporting they have fallen victim to scams and lost money," says ACCC deputy chair, Peter Kell. Almost 70% of people who reported a scam to the ACCC last year said it came via the internet, Kell points out.

In fact, internet fraud is endemic in most developed countries - in the US it raked in almost US\$560 million (\$664 million) last year, more than double the figure from 2008. US researchers say the real number is in the billions of dollars, since it's believed that fewer than one in ten internet crimes gets reported.

Today's scammers practise many cons, some new and some just variations on tried-and-true rip-offs. The big difference is the places they reel in victims. "The rise of social networking sites has created a situation where trust between people can be exploited," says Martin Crocker, the executive director of NetSafe, a New Zealand cyber-security organisation.

Once crooks gain access to a computer (often by enticing the user to click on a link and unwittingly download spyware), they mine it for e-mail addresses and passwords to Facebook, Twitter, and other accounts and pose as members, gaining the trust of friends and family.

Malicious software "robots" lead the charge, but then human crooks in Third World sweatshops take over by typing in the letters of those "captcha" registration boxes (the ones with a jumble of characters that you have to replicate) that thwart mechanised spammers. Then other humans, working out of criminal call centres, communicate with the victim by e-mail or text messaging.

Likely victims include the elderly, who are increasingly comfortable with computers yet tend to be overly trusting. But, surprisingly, young adults fall for scams more than others, says Christine Durst, an internet fraud expert. "They tend to think they're infallible."

Here are some of the latest scams and ways to avoid them. And if you ever get a message from a friend who's stranded in London with no cash, tell her to phone collect so you can hear her voice.

ADDITIONAL REPORTING BY HELEN SANDSTROM

readersdigest.com.au 09/10

## 1 FREE TRIAL OFFER! (Just pay forever)

**>> How it works:** You see an internet offer for a free one-month trial of some amazing product - often a teeth whitener or a weight-loss programme. All you pay is \$5.95 for postage and handling.



that most people don't read all the fine print before clicking on 'I agree', and even people who glance at it just look for numbers. So the companies spell out the numbers, with no dollar signs; anything that has to do with money or a time frame gets washed into the text."

That's exactly what you'll see in the terms for Xtreme Cleanse, a weight-loss pill that ends up costing "seventy-nine dollars ninety-five cents plus five dollars and ninety-five cents shipping and handling" every month once the 14-day free trial period ends or until you cancel.

**>> Avoidance manoeuvre:** Read the fine print on offers, and don't believe every testimonial. Reputable companies will allow you to cancel, but if you can't get out of a "contract", cancel your card immediately, then negotiate a refund; if that doesn't work, appeal to your credit card company.

## 2 THE HOTSPOT IMPOSTOR (He's close, real close)

**>> How it works:** You're sitting in an airport lounge or a coffee shop and you log into the local wi-fi zone. It could be free, or it could resemble a legitimate and familiar pay service. You get connected and everything seems fine.

**>> What's really going on:** Buried in fine print, often in a colour that fades into the background, are terms that obligate you to pay \$79 to \$99 a month in fees, forever.

**>> The big picture:** "Free" trial offers are an emerging problem, according to the ACCC. Last year, reports about online shopping scams, which include free trial offers, increased by more than 100% compared to 2008, says Kell. "These guys are really shrewd," adds Durst. "They know



>> **What's really going on:** The site only looks legitimate. It's actually run by a nearby criminal from a laptop. If it's a "free" site, the crook is mining your computer for banking, credit card and other information. If it's a fake pay site, he gets your purchase payment, then sells your card number to other crooks.

>> **The big picture:** "There's been a growth in wireless hotspots, so people are now accustomed to the idea of being out and accessing the internet from anywhere," says Crocker. But fake wi-fi hotspots can be difficult to tell from the real thing. "It's lucrative and easy to do," says Yoder. "Criminals duplicate the legitimate web page of a wi-fi provider and tweak it so it sends your information to their laptop."

>> **Avoidance manoeuvre:** Make sure you're not set up to automatically connect to non-preferred networks. Before travelling, buy a \$20 Visa or MasterCard gift card to purchase

airport wi-fi access (enough for two days) so you won't broadcast your information. Or set up an advance account at airports you'll be visiting ([travelpost.com](http://travelpost.com) lists wi-fi services at 80 major airports).

Don't do any banking or internet shopping from hotspots unless you're sure the network is secure. And, adds the ACCC, always log out of any programs and erase your search history so the next user cannot access your details.

### 3 THE NOT-SO-SWEET TWITTER TWEET (It's a real long shot)

>> **How it works:** You get a "tweet" from a Twitter follower, raving about a contest for a free iPad or some other expensive prize. "Just click on the link to learn more."

>> **What's really going on:** The link downloads a "bot" (software robot), adding your computer to a botnet of

## How scammers use your credit card

Ever wonder what internet thieves do with all those stolen credit card numbers? One method of converting plastic into big bucks has evolved into its own con game: the re-shipping scam. In this play, scammers enlist innocent people as middlemen in a global fencing operation.

Here's how it happened

to 58-year-old Reba Jowers. Jowers saw an online job ad promising \$500 a week for working at home as a quality control checker. "People ordered a product, and it came to me. I made sure the contents matched the order on the invoice and weren't damaged. Then I'd forward the product to the 'purchaser'," she explains.

It sounded great, so she signed on. Within a week, she started receiving expensive items from online stores like Amazon – high-end digital cameras, binoculars, a watch. But before she even received a mailing list, a credit card company phoned: a customer's card was being used illegally for online



But when users can't see the actual URL, it's easy for bad guys to post malicious links.

>> **Avoidance manoeuvre:** Check website addresses carefully as scammers can set up fake websites with deceptively similar addresses, according to the ACCC.

Before clicking on a Twitter link from a follower you don't know, check out his profile, says Josh George, a website entrepreneur who follows online scams. "If he's following hundreds of thousands of people and nobody is following him, it's a bot," he says.

### 4 YOUR COMPUTER IS INFECTED! (And hey, we can help)

>> **How it works:** A window pops up about a legitimate-sounding antivirus software program such as "Antivirus XP 2010" or

"zombies" that scammers use to send spam e-mail.

>> **The big picture:** Scammers are taking advantage of URL-shortening services that allow Twitter users to share links that would otherwise be longer than the 140-character maximum for a tweet. These legitimate services break down a huge URL to ten or 15 characters.

shopping. Why were the packages being sent to her?

"That put up a big red flag," says Jowers. She e-mailed her "employer" and asked that he stop sending merchandise to her. "He said it had already been shipped to me." When Jowers threatened to call the police, her "employer" reminded

her that she'd signed a contract. If she tried to break it, he said, he'd call the police on her. She contacted the police anyway: they told her to refuse any more shipments. She returned the packages to the shops.

Jowers did not lose any of her own money, but had she continued to participate in the re-shipping scam,

"I probably could have been arrested," she says.

"If police officers follow the goods, in the first instance, they'll reach an innocent victim," says Martin Crocker of NetSafe. "A lot of scams work better if a mule or unsuspecting party is in the middle to help cover the scammer's tracks."



## How to protect yourself

**Don't** use passwords or user IDs that include personal information such as your birth date.

**Don't** use your mother's maiden name as a security question. Pick something more obscure, such as your childhood pet's name.

**Don't** leave passwords in plain view – on your monitor, for example.

**Don't** use the same password for multiple sites. If crooks crack your Twitter account, they can access your bank account, too.

**Do** create passwords that are at least eight to 16 characters long, with a mix of capital letters, numbers and symbols. They're harder to crack.

**Do** use random pattern

codes to create passwords. For example, pick two computer keys – say, 4 and 7. Type straight down the keyboard from 4 until you reach the bottom (the letter V), then type one character to the left. Then do the same for 7, this time using all caps.

You now have a meaningless password that reads 47fvc7UJMN, but all you have to remember is 47. Or use the first letter of each word in a line from a favourite song or poem.

**Do** change passwords often, about once a month.

**Do** hold your cursor over an unknown link before clicking on it, and look at the bottom of your web browser. It will show

where the link is actually taking you to.

**Do** note the wording before the .com, .com.au, .org.au (or similar) part of the URL. It's what counts. So while paypal.com is legitimate, paypal.1234.com is fake.

**Do** look out for links with the @ symbol. Browsers ignore everything to the left of it, so paypal@1234.com is not a PayPal site.

**Do** watch for deliberate misspellings – such as paypal.com – designed to trick you into clicking.

**Have a scam to report?**

Visit the ACCC's SCAMwatch site – scamwatch.gov.au – or call the SCAMwatch hotline on 1300 795 995.

advantage of the smartphone revolution – hoping that a text message to your mobile phone will make it less likely you'll investigate the source, as you might do while sitting at your desk. Since many banks and businesses do offer text-message notifications, the scam has the air of legitimacy.

Shirena Parker, a 20-year-old newlywed, was thrilled when she got a text message announcing she'd won a \$250 gift card. When she called the number, a representative explained

there would be a \$2 postage charge (later upped to \$4 by another "representative"). Parker gave the scammer her debit card number and started getting round-the-clock calls from him, asking for the phone numbers and e-mails of friends and family. "It was turning into harassment," she says. After two days, she discovered the shop was not giving away gift cards. Hearing that, Parker's husband cancelled their debit card before the scammers could empty the account

"SecurityTool", alerting you that your machine has been infected with a dangerous bug. You're prompted to click on a link that will run a scan. Of course, the virus is found – and for a fee, typically about \$50, the company promises to clean up your computer.

**>> What's really going on:** When you click on the link, the bogus company installs malware – malicious software – on your computer. No surprise, there will be no clean-up. But the thieves have your credit card number, you've lost the money, and your computer is left on life support.

**>> The big picture:** Bogus security software, or "scareware", is not new to Australians, but scammers are getting bolder and are now cold-calling people and scaring them into believing their computer is infected. The caller claims to be a representative from Microsoft or another genuine service provider and requests remote access to your computer to check if it has been infected with a virus.

"This scam has the potential to work because the victim may let down their guard when told by the offender they have specific knowledge of error messages on their system," says Detective Superintendent Brian Hay of Queensland's State Crime Operations Command Fraud and Corporate Crime Group. "This gives the victim confidence in the caller, which opens the door to fraud."

56

readersdigest.com.au 09/10

**>> Avoidance manoeuvre:** If you get a pop-up virus warning, close the window without clicking on any links. Then run a full system scan using legitimate, updated antivirus software.

If you receive a phone call out of the blue from someone about your computer system's security status, hang up and never give a stranger remote access to your computer.

## 5 DIALLING FOR DOLLARS (With a ring of fraud)

**>> How it works:** You get a text message on your mobile phone from your bank or credit card issuer: there's been a problem, and you need to phone right away with some account information. Or the message says you've won a gift certificate to a chain store – just call the free number to get yours now.

**>> What's really going on:** The "bank" is a scammer hoping you'll reveal your account information. The gift certificate is equally bogus; when you call the number, you'll be told you need to subscribe to magazines or pay shipping fees to collect your prize. If you bite, you will have surrendered your credit card information to marketers who will ring up false charges.

**>> The big picture:** Welcome to "smishing", which stands for "SMS phishing", the new, text-message version of the lucrative e-mail scam. In this ploy, scammers take



but not before they had helped themselves to the \$4 "postage" fee.

"I don't know how they got my name and phone number," says Parker. "But I learnt my lesson."

**>> Avoidance manoeuvre:** Real banks and shops might send you notices via text message (if you've signed up for the service), but they never ask for account information. If you're unsure, call the bank or shop directly. You can also Google the phone number to see if any scam reports turn up. Had Parker checked out the phone number, she would have learnt this was a scam.

## 6 WE ARE THE WORLD (The world of charity scams, that is)

**>> How it works:** You get an e-mail with an image of a malnourished orphan - from Haiti or another developing nation. "Please give what you can today," goes the e-mail's plea, followed by a request for cash. To speed relief efforts, the e-mail recommends you send a Western Union wire transfer as well as information such as your address and your bank account numbers.

**>> What's really going on:** The "charity" mailing is a scam designed to harvest your cash and banking information. Nothing goes to helping disaster victims.

**>> The big picture:** The internet, e-mail and text messaging have given new life to age-old charity scams.

These con artists watch the

headlines very closely, and they quickly set up fake websites and

PayPal accounts to take advantage of people's kindness and sympathy. The ACCC reports this year's Haiti earthquake, the 2009 Victorian bushfires and the 2004 Asian tsunami all triggered online charity scams.

**>> Avoidance manoeuvre:** Donate to real charities on their own websites, rather than clicking on links in e-mail solicitations. Genuine aid organisations will accept donations by credit card or cheque; they won't ask for wire transfers or bank account information.

## 7 TRUE LOVE FOR SALE (The cruellest con)

**>> How it works:** You meet someone on a dating site, on Facebook, or in a chat room. You exchange pictures, talk on the phone. It soon becomes obvious that you were meant for each other. But the love of your life lives in a foreign country and needs money to get away from a cruel father, or to get medical care, or to buy a plane ticket so you can finally be together.

**>> What's really going on:** Your new love is a scam artist. There will be no tearful hug at the airport, no happily-ever-after. You will lose your money.

**>> The big picture:** Online social networking has opened up new paths for heartless scammers who specialise in luring lonely people into bogus love affairs

or friendships, only to steal as much of their money as they can.

"Not as many people fall for this type of scam, but when they do the quantities of money handed over can be extraordinary," says Crocker. "[In terms of time] it's a high investment from the scammer, but it's also a high return when it works."

Cindy Dawson, a 39-year-old customer service representative, fell for a Nigerian named Simon Peters whom she met on a dating site. "We started talking on the phone," the divorced mother of three recalls. They exchanged photos; Peters was a handsome man. Dawson sent him pictures of her kids. "He kept saying how much he cared about me," says Dawson, fighting back tears at the memory. "I was in love with him."

Soon enough, Peters started asking for money - small amounts at first, to buy food. He always wanted the money wired by Western Union to someone named Adelwale Mazu. Peters said he couldn't use his own name because he didn't have the right documentation. "It started progressing to higher amounts of money," says Dawson. "I sent him money for an airfare from Nigeria. I

drove to the airport, but he never turned up." Peters continued working the scam, explaining that authorities in Lagos wouldn't let him board the plane. Then he needed money to study. Then he was stuck in London. "Everybody told me he was scamming me," says Dawson, "but I didn't want to believe it. Finally my 12-year-old daughter said, 'Stop sending him money; he's never coming.'"

After reading more about this type of con on *romancescams.org*, Dawson searched for the fake name and discovered that Peters's photo was a stock image of a male model copied from the web. "He got about \$15,000 out of me," Dawson confesses. "I was angry, and I felt stupid."

**>> Avoidance manoeuvre:** "On the internet, it is almost impossible to be too paranoid," says Durst. Dating and social-networking sites can be a great way to meet new friends. But if someone you know only from the internet asks for money, sign off quickly.

**Have you ever been ripped off by an online scam? Tell us and other readers how it happened at [readersdigest.com.au/contribute](http://readersdigest.com.au/contribute) or see page 8 for details.**

